DOCKET NO: 203223US-28

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF	:
SHINGO YAMAGUCHI	: EXAMINER: HA, L.
SERIAL NO: 09/863,384	:
FILED: MAY 24, 2001	: GROUP ART UNIT: 2135
FOR: METHOD AND SYSTEM FOR CONTROLLING ACCESS TO NETWORK RESOURCES BASED ON CONNECTION SECURITY	:

APPEAL BRIEF

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

Applicants appeal the outstanding Final Rejection of April 6, 2006.

I. REAL PARTY IN INTEREST

The real party in interest in the present application is the assignee of the present application, Ricoh Co., Ltd., having a place of business at 3-6 Nakamagome 1-chome, Ohta-ku, Tokyo 143-8555, Japan.

II. RELATED APPEALS AND INTERFERENCES

Appellant, Appellant's legal representative, and the assignee are not aware of any prior and pending appeals, interferences, or judicial proceedings that may be related to, directly effect or be directed effected by, or having a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 41-43, 45, 50-63, 65, and 70-80 are pending in this application. Each of those claims is rejected and is being appealed.

Claims 1-40, 44, 46-49, 64, and 66-69 were canceled during prosecution of the present application.

IIII. STATUS OF AMENDMENTS

No amendment was filed subsequent to the Final Rejection of April 6, 2006.

IV. SUMMARY OF CLAIMED SUBJECT MATTER

The present invention is directed to controlling the level of access to network resources, connected to a network, based on a level of security of a connection to the network.[1]

As shown in Figure 1A in the present specification as a non-limiting example, different computing devices 2, 6 can be connected to an intermediate device 10. The claimed invention has as an operation to control the access of those computing devices 2, 6 to resources on the network 12A based on how the computing devices 2, 6 connect to the intermediate device 10. With reference to Figure 2A in the present specification as a non-limiting example, if either of the computing devices 2, 6 connect to the intermediate device 10 through an encrypted connection, driver 54 is activated and a firewall setting for level 1 access is provided. In that case a high level of access to various network resources, including a file server, can be provided.[2] Alternatively, if no encryption is utilized for the connection between either of the computing devices 2, 6 and the intermediate device 10, the driver 56 is

[1] Specification at paragraph [0001].
[2] Specification at page 6, lines 10-15, paragraph [0023].

activated and a firewall setting for level 2 access is utilized. In that case a user may only have a limited access to resources, including the Internet and an email server, on the network.[3] In both cases the user has access to network resources, but that access is more restricted for the level access.

In such ways, in the claimed invention, a security level of a network connection between the computing device and the intermediate device can control the level of network resources available to the computing device.

With respect to the claims, the claims are directed to a method of controlling a network and a system for controlling a network. In the method and system a computer network connection is established between a computing device and an intermediate device that has network resources connected thereto. The corresponding element to the "means for establishing a computer network" is the intermediate device 10 shown for example in Figures 1A, 2A, 2B, and 3 in the present specification, or in a further embodiment the login server 30, or in a further embodiment the firewall device 140 shown in Figure 5, see also the present specification at paragraphs [0017], [0032], [0033].

Further, a level of security in the computer network connection is determined based on whether the computer network connection to connect the computing device to the intermediate device is encrypted, such that a first level of security is set when it is determined that the computer network connection is encrypted and a second level of security is set when it is determined that the computer network connection is not encrypted. The element corresponding to the "means for determining a level of security" is the intermediate device 10, and with reference to Figures 2A and 2B in the present specification see the Driver For Wireless LAN Card 54 (Encryption) and the Driver For Wireless LAN Card 56 (No Encryption), operating in conjunction with the Firewall Setting for Level 1 (62) and the

[3] Specification at page 6, lines 15-26, paragraph [0023].

Firewall Setting for Level 2 (64), and step 106 in Figure 4, and see also the present specification at paragraphs [0022]-[0023]. In alternate embodiments see also the login server 30 and firewall device 140, paragraphs [0032], [0033].

Further, a level of access of the computing device to the network resource is controlled using the level of security of the computer network connection that has been determined, such that the computing device is only allowed access to a first set of network resources, including a file server, based on the determined first level of security, and is not allowed access to the first set of network resources, but is allowed access to a second set of network resources, including access to the Internet and an e-mail server, based on a determined second level of security. With respect to the "means for controlling a level of access of the computing device" see the intermediate device 10, and particularly the firewall device 58 in Figures 2A and 2B and step 108 in Figure 4 of the present specification, see also the present specification at paragraphs [0023] and [0024]. In an alternative embodiment see the login server 30 and the present specification at paragraph [0031]. As another alternative embodiment see the firewall device 140 in Figure 5 and the present specification at paragraphs [0033]-[0034].

V. GROUNDS OF REJECTION

Claims 41-42, 44, 46-62, 64, and 66-80 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. patent 6,453,419 to Flint et al. (herein "Flint") and further in view of U.S. patent 6,609,198 to Wood et al. (herein "Wood"). Claims 43, 45, 63, and 65 were rejected under 35 U.S.C. § 103(a) as unpatentable over Flint and Wood and further in view of the Microsoft Computer Dictionary, 5th Ed. (herein "Microsoft Dictionary").

Each of the above-noted rejections is being appealed.

VI. ARGUMENT

Applicants respectfully submit the claims as currently written clearly recite features that are not taught or suggested by the applied art, and that have not been properly considered in the Office Action.

Independent claim 41 recites determining the level of security of the computer network connection based on whether the computer network connection is encrypted, and "wherein a first level of security is set when it is determined that the computer network connection is encrypted and a second level of security is set when it is determined that the computer network connection is not encrypted". Independent claim 41 also recites that a level of access of the computing device to the network resources is controlled such that the computing device is only allowed access to the first set of network resources, which include a file server, when the first level of security, i.e. an encrypted connection, is determined, and is not allowed access to the first set of network resources but is allowed access to the second set of network resources, which include access to the Internet and an email server, when a second level of security, i.e. a non-encrypted connection, is determined. Independent claim 61 also recites similar limitations.

Flint is cited as the primary reference with respect to certain above-noted claim features. However, applicants respectfully submit Flint does not disclose or suggest the above-noted features in independent claims 41 and 61. Flint merely discloses that a non-encrypted connection can result in ***no access to a computer network***. The claims have a different structure in that in the claims a non-encrypted connection still gives rise to access to resources on the network, including the Internet and an email server.

In further detail, Flint discloses the use of a filter 72, see Figure 4. Flint discloses that the filter can be an encryption filter and "the encryption filter requires that a connection is encrypted with a certain level of encryption. It will be up to the user level process to verify

that the requirements of the filter are met. If the requirements are not met the ***action is to deny the connection***". (Flint at column 11, lines 58-62, emphasis added).

From the above-noted disclosure it is clear that in Flint the filter is provided to merely deny a connection to a network for example if an encryption connection is not utilized.

The claims recite a different operation than that in Flint. In the claims connection to a network can still be provided even if a lower level non-encrypted connection is utilized. However in the claims such a lower level non-encrypted connection results in a different level of access to network resources.

Features recited in independent claims 41 and 61 are allowing access to a file server if an encrypted connection is made, and not allowing access to the file server but allowing access to the Internet and an e-mail server if a non-encrypted connection is made. Flint fails to teach or suggest such features.

Flint, at col. 3, line 48 to col. 4, line 1 and col. 11, lines 58-59, Flint merely discloses the use of firewalls and encryption. However, at no point does Flint disclose or suggest the features recited in the claims in which when a connection to a computer network is via an encrypted connection, the connecting device can access first resources including a file server, but when the connecting device connects via a non-encrypted connection, the connecting device can access second network resources including the Internet and the email server, and cannot access the first set of resources, i.e. cannot access the file server.

The Final Rejection also appears to cite Flint at column 5, lines 39-40 and column 12, lines 13-15 as meeting the claim limitation that a computing device is allowed access to a first set of network resources including a file server based on a determined first level of security, and is not allowed access to the first set of network resources but is allowed access

to a second set of network resources, including access to the Internet and the e-mail server, based on a determined second level of security.[4]

Applicants traverse the above position as now discussed.

At column 5, lines 39-40 Flint merely makes a broad reference to the Internet and states "In FIG. 5, rule 61 manages HTTP and SSL connections over the Internet". That disclosure in Flint is completely unrelated to how to access the Internet. The Final Rejection has merely found the term Internet in the reference to Flint and applied the term to the claims without any recognition of what the claims actually recite. The noted disclosure in Flint does ***not*** indicate that access to the Internet is controlled based on an encrypted or non-encrypted connection to a network. Merely because Flint utilizes the word "Internet" does not indicate Flint meets the claim limitations. The outstanding Final Rejection has not considered the claimed features in that respect.

Further, at column 12, lines 13-15 Flint also merely utilizes the word "e-mail", although at that portion with respect to an e-mail filter. Again that disclosure in Flint is not directed to the claimed features. In the claims an e-mail server can be accessed when a non-encrypted connection is made to a network. Flint does not disclose any even closely related feature.

Moreover, applicants note the Final Action has not even attempted to indicate how the features recited above, that when an encrypted connection is made to a network access to a file server is granted, is met by Flint. The Final Action has not even attempted to point to any element in any reference to meet that claim feature.

According to features recited in the claims, if an encrypted connection is made from a computing device, that computing device can have access to a first level of network resources, including a file server. If a second non-encrypted connection is made by the

[4] Final Office Action of April 6, 2006, page 3, middle paragraph.

computing device, that computing device only has a more limited access to a second set of network resources, including access to the Internet and an email server.

The relied upon disclosures in Flint do not even address such claimed features.

Moreover, applicants respectfully submit no teachings in Wood cure the deficiencies in Flint.

Wood is even directed to a completely different device than in Flint. That is, Wood is directed to a device that allows multiple accesses to a network based on trust-levels. Flint is not directed to any such type device.

Addressing now the "Response to Arguments" section in the Final Action, that section does not provide any comments that would properly support the rejection. In maintaining the rejection the Final Action summarizes the "Response to Arguments" section as follows:

> Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Flint to include allowing access to a first set of resources based on the first level of security and allowing access to a second set of resources based on the determined second level of security as taught by Wood [COL. 8, lines 23-46], because this allows an entity to tailor its credentialing to current access requirement and is more difficult to maintain a uniform security policy across a set of resources [COL. 1, lines 58-62 and COL. 2, lines 61-63].[5]

In reply to the above-noted statement, applicants note the basis for the outstanding rejection ***has not considered all the claimed features***. The claims do not broadly recite allowing access to a first set of resources based on a first level of security and allowing access to a second set of resources based on a second level of security. The claims more specifically recite when the first level of security, which is an encrypted connection, is met a computing device can have access to a file server, and when a second level of security is met, which is a non-encrypted connection, the computing device is not allowed access to the first

[5] Final Office Action of April 6, 2006, page 18, bottom paragraph.

set of network resources, i.e., is not allowed access to the file server, but is allowed access to the Internet and an e-mail server. The claims are more specific than as addressed in the Office Action.

The basis for the outstanding rejection simply has not even addressed the claimed features noted above.

In such ways the combination of teachings of Flint and Wood, does not meet limitations recited in the claims as currently written.

Moreover, no teachings in the Microsoft Dictionary were cited with respect to the above-noted claim limitations, or are believed to cure the deficiencies of Flint in view of Wood.

VII. CONCLUSION

In view of the foregoing comments applicants respectfully submit the outstanding rejections must be REVERSED.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

James J. Kulbaski
Attorney of Record
Registration No. 34,648

Surinder Sachar
Registration No. 34,423

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 03/06)

I:\ATTY\SNS\20's\203223\203223US-AB.DOC

APPENDIX

Claims 1-40 (Canceled).

Claim 41: A method of controlling a network, comprising:

establishing a computer network connection between a computing device and an intermediate device that has network resources connected thereto;

determining a level of security of the computer network connection based on determining whether the computer network connection to connect the computing device to the intermediate device is encrypted, wherein a first level of security is set when it is determined that the computer network connection is encrypted and a second level of security is set when it is determined that the computer network connection is not encrypted; and

controlling a level of access of the computing device to the network resources using the level of security of the computer network connection that has been determined, such that the computing device is allowed access to a first set of network resources, including a file server, based on a determined first level of security, and is not allowed access to the first set of network resources but is allowed access to a second set of network resources, including access to the Internet and an email server, based on a determined second level of security.

Claim 42: A method according to claim 41, wherein said establishing comprises:

establishing a wireless computer network connection.

Claim 43: A method according to claim 41, wherein said establishing the wireless computer network connection comprises:

establishing a wireless computer network connection which conforms to an IEEE 802.11b standard.

Claim 44 (Canceled).

Claim 45: A method according to claim 44, wherein said determining whether the computer network connection is encrypted comprises:

determining whether the computer network connection is encrypted using Wired Equivalent Privacy ("WEP") encryption.

Claims 46-49 (Canceled).

Claim 50: A method according to claim 41, wherein:

said determining is performed by the intermediate device, and

said controlling is performed by the intermediate device.

Claim 51: A method according to claim 50, wherein:

said determining is performed by the intermediate device which is a router.

Claim 52: A method according to claim 51, wherein:

said controlling is performed by the intermediate device which is a router having a firewall operation.

Claim 53: A method according to claim 52, wherein:

said establishing is performed using the intermediate device which is a router which establishes a wireless connection to the computer.

Claim 54: A method according to claim 41, wherein:

said determining is performed by a server running a network operating system, the server being different from the intermediate device, and

said controlling is performed by the server running the network operating system.

Claim 55: A method according to claim 54, wherein:

said determining is performed by the server which is running a network directory service.

Claim 56: A method according to claim 54, wherein:

said establishing is performed by a bridge connected to the computer through the computer network connection.

Claim 57: A method according to claim 56, wherein:

said establishing is performed by the bridge connected to the computing device through the computer network connection which is a wireless network connection.

Claim 58: A method according to claim 41, wherein said controlling comprises:

controlling the level of access by a stand-alone firewall device which is connected between the intermediate device and the network resources.

Claim 59: A method according to claim 58, wherein said determining comprises:

determining the level of security using the intermediate device.

Claim 60: A method according to claim 58, wherein said establishing comprises:

establishing the computer network connection as a wireless connection using the intermediate device.

Claim 61: A system for controlling a network, comprising:

means for establishing a computer network connection between a computing device and an intermediate device that has network resources connected thereto;

means for determining a level of security of the computer network connection based on determining whether the computer network connection to connect the computing device to the intermediate device is encrypted, wherein a first level of security is set when it is determined that the computer network connection is encrypted and a second level of security is set when it is determined that the computer network connection is not encrypted; and

means for controlling a level of access of the computing device to the network resources using the level of security of the computer network connection that has been determined, such that the computing device is only allowed access to a first set of network resources, including a file server, based on a determined first level of security, and is not allowed access to the first set of network resources but is allowed to access to a second set of network resources, including access to the Internet and an email server, based on a determined second level of security.

Claim 62: A system according to claim 61, wherein said means for establishing comprises: means for establishing a wireless computer network connection.

Claim 63: A system according to claim 61, wherein said means for establishing the wireless computer network connection comprises:

means for establishing a wireless computer network connection which conforms to an IEEE 802.11b standard.

Claim 64 (Canceled).

Claim 65: A system according to claim 64, wherein said means for determining whether data from the computing device is encrypted comprises:

means for determining whether the computer network connection is encrypted using Wired Equivalent Privacy ("WEP") encryption.

Claims 66-69 (Canceled).

Claim 70: A system according to claim 61, wherein:

said means for determining is the intermediate device, and

said means for controlling is the intermediate device.

Claim 71: A system according to claim 70, wherein:

said means for determining is the intermediate device which is a router.

Claim 72: A system according to claim 71, wherein:

said means for controlling is the intermediate device which is a router having a firewall operation.

Claim 73: A system according to claim 72, wherein:

said means for establishing is the intermediate device which is a router which establishes a wireless connection to the computer.

Claim 74: A system according to claim 71, wherein:

said means for determining is a server running a network operating system, the server being different from the intermediate device, and

said means for controlling is the server running the network operating system.

Claim 75: A system according to claim 74, wherein:

said means for determining is the server which is running a network directory service.

Claim 76: A system according to claim 74, wherein:

said means for establishing is a bridge connected to the computer through the computer network connection.

Claim 77: A system according to claim 76, wherein:

said means for establishing is the bridge connected to the computer through the computer network connection which is a wireless network connection.

Claim 78: A system according to claim 61, wherein said means for controlling comprises:

a stand-alone firewall device which is connected between the intermediate device and the network resources.

Claim 79: A system according to claim 78, wherein said means for determining comprises:

means for determining the level of security using the intermediate device.

Claim 80: A system according to claim 78, wherein said means for establishing comprises:

means for establishing the computer network connection as a wireless connection using the intermediate device.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.